

# 新一代互联网体系结构

陆璇, 龚向阳, 程时端

(北京邮电大学 网络与交换技术国家重点实验室, 北京 100876)

**[编者按]** 互联网目前面临着各种问题和挑战, 其体系结构再次成为了网络领域研究的热点之一。本讲座将分为3期介绍互联网体系结构的研究现状及未来的展望。第1期介绍目前互联网体系结构面临的挑战以及国内外的研究现状。第2期将介绍现有互联网体系结构向新一代互联网体系结构演进中的关键技术与解决方案, 内容涉及新型路由寻址体系结构、端到端原则、网络安全性与可信性等方面的研究。第3期将介绍以全新的革命性方式来解决当前互联网体系结构缺陷的新一代互联网体系结构, 包括国内外的研究现状和主要的解决方案, 并对新一代互联网体系结构的研究进行了展望和总结。

中图分类号: TP393.4 文献标识码: A 文章编号: 1009-6868 (2009) 04-0057-04

## 1 当前互联网的体系结构以及面临的挑战

经过多年发展, 互联网已经取得了巨大的成功, 成长为一个全球性的信息系统。但是随着互联网的普及、商业化以及新业务的不断涌现, 其各种先天不足和缺陷也日益明显地暴露出来, 例如IP地址匮乏、缺乏服务质量(QoS)与安全保障机制、路由系统扩展性低等。传统互联网指数增长的复杂度也使得网络控制和管理十分困难, 难以满足多样化的应用需求。尽管研究人员已经提出了多种解决方案试图对传统互联网进行改进, 例如引入网络地址转换(NAT)、集成服务模型/区分服务模型(IntServ/DiffServ)、防火墙、IPSec等来解决上述的问题, 但这些方案都未能从根源上解决当前互联网所面临的核心问题——当前互联网的体系结构存在着难以克服的缺陷。为此, 大量

研究机构开始重新考虑和研究互联网的体系结构, 试图提出适应于未来环境和应用需求的新型互联网体系结构。新型的网络体系结构必须能够支持融合的异构网络环境、支持各种新的网络功能、新型应用和新型计算技术。新一代互联网环境对体系结构的需求如图1所示。

### 1.1 互联网的体系结构

互联网体系结构是指导互联网设计的一系列抽象设计原则, 内容涉及互联网的构成要素、通信协议、网络功能以及管理运营方式等。互联网

体系结构设计的合理性将对互联网的网络性能、服务提供以及是否支持持续化的演进产生决定性影响。

在网络体系结构的设计中, 国际标准化组织/开放系统互联模型(ISO/OSI)是一个重要的理论指导。而在互联网中, TCP/IP协议采用了更简洁和高效的体系结构, 这种基础结构以及Web等应用技术的出现使得互联网获得了巨大成功。当前互联网已经发展为拥有超过数亿台主机的复杂的超级信息系统。互联网的成功, 主要归功于它在体系结构设计时所遵守的一系列基本原则: 如开放性原则、端到端原则、透明性原则、分层原则、尽力而为原则等。但是, 当前的应用需求与网络环境已经与传统互联网的设计目标发生了巨大变化。传统互联网原有的一些设计原则已成为阻碍互联网进一步发展的主要障碍。因此, 新一代互联网体系结构的研究中, 既需要总结和继承传统互联网的成功经验, 也需要在研究未来互联网体系结构所面临的挑战的基础上, 重新审视和确定新一代互联网体系结构设计原则与方法。

### 1.2 当前互联网体系结构面临的问题与挑战

互联网最初是为单一的数据通信需求而设计的, 其设计目标是实现网络的健壮性和支持底层网络技术的异构性, 并且默认互联的用户属于相互信任的团体。因此, 传统的互联网体系结构仅支持尽力而为的服务,

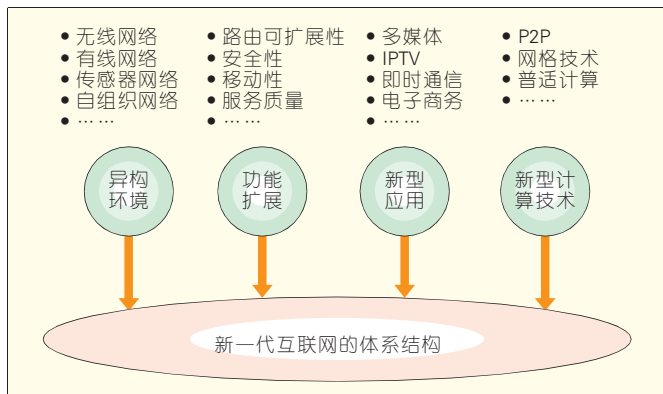


图1 新一代互联网体系结构的需求

**基金项目:** 国家高技术研究发展计划(“863”计划)资助项目(2007AA01Z206); 北京重点学科建设项目(key disciplines)

遵循“核心简单,边缘智能”的设计原则,网络智能部署在网络边缘的终端上。这种体系结构简单,但保证了高效的互通和良好的演进性,并且一直沿用至今。

然而近年来,随着网络技术的高速发展,出现了大量新型接入技术如WiMAX、Wi-Fi、无线局域网、蓝牙,大量新型异构网络如移动自组织网络、无线传感器网络、网状网,大量新的计算技术如P2P、网格、普适计算和多样化的应用,这些新技术和应用在推动整个通信领域进步的同时,也使得传统互联网体系结构面临着巨大的挑战。复杂的异构网络环境增加了维护管理的复杂度,同时也影响了网络的灵活性、健壮性和安全性;无处不在的应用需求要求互联网支持移动性;多样化的应用要求互联网支持不同实时性的业务。随着网络复杂度的增长,传统的“核心简单”的互联网难以满足网络对可控、可管迫切的需求,具体分析其原因,可以发现当前互联网体系结构所存在的问题与挑战。

#### (1)端到端原则和中间盒

端到端原则将网络智能推向边缘,减少通信子网冗余和复杂性,核心网只提供高效的数据传输功能。然而由于种种原因,该原则并未被完全遵守。为了弥补互联网体系结构的不足,网络中常常引入各种类型的中间盒,例如NAT、防火墙、代理等。这些中间盒的引入都违背了端到端原则,使网络失去了端到端透明性,导致了更加复杂的网络管理和配置,并可能造成安全漏洞和故障率的增加。

#### (2)路由、寻址与移动性问题

为解决IPv4地址即将耗尽的问题,互联网工程任务组(IETF)相继提出了无类域间路由(CIDR)、NAT和IPv6等方案。由于IPv6与IPv4的互通问题,IPv6的部署进程较缓慢。NAT从短期来看解决了IP地址不足的问题,无需修改现有主机和路由器,部署方便,因而得到了广泛应用。但是从长

期来看,NAT在端对端应用、主机与IP地址捆绑、网络管理方面都存在无法克服的弊端,并非是一种最终的解决方案。网络多归属、流量工程以及运营商独立(PI)地址的广泛应用造成了路由的扩展性问题。新兴的普适计算要求网络能给用户提供无处不在、无处不在、无所不有的综合性服务,而移动性是必须满足的基本需求之一。但是传统互联网从本质上不支持连接过程中IP地址的动态变化,导致主机移动的同时连接无法维持,难以满足用户对移动实时业务的需求。这些问题都需要在未来互联网体系结构设计中解决。

#### (3)安全性和可信性

早期的互联网被默认为“安全的网络”,因为传统互联网默认其用户群体主要是彼此相互信任、目标一致的团体,安全问题未得到设计者的重视。但是随着互联网的商用化和全球爆炸式发展,其用户群体在规模、目标、素质等方面各不相同,用户间的信任不复存在。互联网上病毒、网络攻击频繁发生,隐私无法保证,互联网被默认为“不安全的网”。尽管学术界和工业界提出了一些解决方案(其中一些已经得到了应用),由于原有互联网体系结构缺乏整体安全框架,各种安全技术以“补丁”方式添加,难免出现安全漏洞或功能重叠,甚至顾此失彼。

#### (4)服务质量

传统互联网体系结构中核心网络只保存有限的管理信息,不提供QoS保证。随着互联网的商业化,大量实时应用涌现出来。视频会议和IPTV等多媒体应用对延迟、延迟抖动、带宽等有严格的需求,需要网络提供相应的服务质量保证。现有的QoS保障模型如IntServ/DiffServ、多协议标签交换(MPLS)、QoS路由等,由于也属于以“补丁”形式加入到网络体系结构中,在实际的应用与部署中存在一些问题。例如,IntServ扩展性差和管理开销大;DiffServ则无法为每个数据流提

供QoS保障。

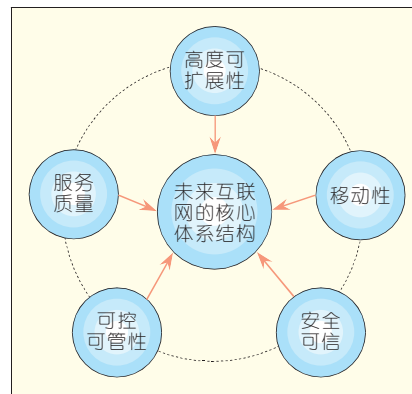
#### (5)网络控制、管理

种类繁多的新型应用和多种新技术的引入,以及网络环境的动态变化,大大增加了网络管理与控制的复杂性。实现对网络的可控可管是未来互联网设计的一项紧迫需求。然而传统互联网体系结构的设计理念使得网络中缺乏用于网络控制管理的必要信息,难以实现高效的网络管理和控制。

为了解决现有互联网存在的问题,满足和适应当前及未来的网络应用对互联网的多样化需求,研究和建设新一代互联网体系结构已经是一项迫在眉睫的任务。新一代互联网技术研究的中心问题是提出一种高效、大规模、高度可伸缩、支持异构网络技术融合的基础网络体系结构。新一代互联网体系结构的设计目标如图2所示,该体系结构的设计将支持移动性、QoS保障、安全性和可信性,以及网络的可控可管。

## 2 未来互联网体系结构的研究现状

近年来,国内外研究机构对未来互联网体系结构进行了大量积极的探索和研究。对于如何解决当前互联网所面临的问题与挑战,研究和建设新一代互联网体系结构,学术界和工业界目前存在着两种观点。第一种观点是采用演进方案,即继续沿用现有互联网体系结构,并以此为基础对现



▲图2 下一代互联网体系结构的设计目标

有网络进行逐步演进和发展,添加新的功能和特性来解决目前面临的问题,满足未来互联网的应用需求。例如,在传统互联网体系结构中添加支持移动性、安全性等的组件。这种方法易于部署和实施,有利于保护现有互联网建设中的已有投入,但是传统互联网体系结构中的一些固有问题难以得到根本性的解决。另一种观点认为,目前正是互联网体系结构进行全面彻底变革的好时机,应该“从零开始”,完全舍弃现有的互联网体系结构,设计一种全新的、融合多种设计目标的新一代互联网体系结构。这种方案旨在从根本上解决现有互联网体系结构存在的各种问题,是一种革命性的方案,但是由于全新网络可能不能兼容现有互联网,需要完全替换原有网络的基础设施,因此存在着网络部署和平滑过渡的问题。

### 2.1 基于现有互联网体系结构的演进

为了解决目前互联网面临的问题并使其能适应未来的发展,持有第一种观点的研究人员提出了一些解决方案,主要是基于现有的互联网体系结构(TCP/IP协议栈),提出一些新的协议或是对一些原有协议和机制进行完善和更新,也就是所谓的演进方案。一般说来,这些协议仅关注互联网体系结构中的某个或某几个问题,包括路由的可扩展性、端到端原则的争论、网络的安全性和可信性,以及网络的自治特性等。

为解决路由的可扩展性问题,学术界进行了对新一代路由寻址架构的探索。美国加州大学Lon Stoica等人在2002年在美国计算机协会数据通信专业组(ACM SIGCOMM)上首先提出了因特网间接访问基础架构(I3)体系结构。以I3为基础,随后又出现了一系列改进的方案,如麻省理工学院的Hari Balakrishnan在2004年发表的互联网分层命名结构(LNAI)以及Matthew Caesar等人在2006年提出的扁平标签路由(ROFL)。这些方案都采用了身份

标识和位置标识的分离,并研究了采用基于身份标识的路由机制的可行性。与此同时,工业界也对此表现出了浓厚的兴趣。Cisco和Ericsson等设备厂商分别对身份标识和位置标识分离的路由体系投入大量人力进行相关研究。Cisco在互联网研究任务组路由工作组(IRTFRRG)提出了位置与标识分离协议(LISP),解决了路由的可扩展性问题,同时最大限度地考虑了网络的可演进性。Ericsson继2000年提出主机标识协议(HIP)以来,在这个研究课题上持续投入,不断完善HIP相关技术体系,并在IETF和IRTFRRG分别成立HIP工作组和HIP研究组进行HIP相关的研究和标准化工作。

关于端到端原则的争论也是互联网体系结构研究中的一个重要议题。Internet之父D. Clark在中指出端到端原则仍然正确,但同时也承认它需要一个更加复杂并且清晰的表述。端到端原则的一个最大缺点就是导致网络中的主机容易受到入侵。虽然目前NAT和防火墙可以起到一定的保护作用,但它们只在目的网络的边缘路由器起作用,恶意数据包仍然消耗了中间链路和中间结点的带宽、资源。所以,有人提出了一个简单的方法来实现网络安全:采用“默认不可达”通信模型来取代“端到端”模型;网络结点在默认情况下是不可达的,除非这种可达性被目的结点明确的允许。

网络的安全性和可信性是新一代互联网体系结构中又一个必须解决的问题。目前解决网络安全的方案可分为3类:在协议栈中增加一个“安全层”;协议栈各层分别设计安全机制,如IPSec主要是增强IP层的安全性;借鉴系统可信性的概念,构建可信网络体系结构,从根本上解决网络的安全性问题。在中国,国家自然科学基金、国家“973”和“863”等项目已经投入了大量经费资助针对可控、可信、可扩展的新一代互联网体系结构方面的研究。

目前互联网的运营和维护需要极大的管理开销和人工干预。针对这一问题,网络自治的概念被引入到互联网体系结构的设计中。欧盟在2008年启动了信息通信领域(ICT)第七框架计划(FP7)研究项目EFIPSANS,其参与者包括设备厂商、大学和科研机构。该项目的目标是在IPv6的基础上设计和构建自治网络和服务,目前已经提出了一个通用的自治网络体系结构。

近10年以来,中国的科研工作者在国家自然科学基金、“973”和“863”项目的支持下,开展了互联网的演进和发展的研究。2003年国家发展改革委等八部委联合组织,启动了我国下一代互联网示范工程(CNGI),目标是搭建下一代以IPv6为核心的互联网实验平台。2007年国家“863”重大项目“新一代高可信网络”、2007年国家“973”项目“可测可控可管的IP网的基础研究”等都充分显示了中国对于互联网的演进和发展研究的重视。

### 2.2 全新的互联网体系结构设计

在互联网体系结构的研究领域中,存在着第二种学术观点,即革命的观点。这个观点主张设计一个全新的网络体系结构,从根本上解决当前互联网面临的各种问题,并适应未来发展的需要。显然,这个网络应具有可扩展性、灵活性、鲁棒性、异构性、可控可管性、安全可信等特征。

近年来,美国和欧洲相继启动了一批未来互联网的研究项目,包括美国的未来互联网体系结构(NewArch)、全球网络创新环境(GENI)和未来互联网设计(FIND)以及欧盟的自治网络体系架构(ANA)、生物学启发的自治网络和服务(BIONETS)、Haggle项目等等。

NewArch启动于2000年初,是由美国美国国防部高级研究规划局(DARPA)赞助,美国国会信息研究院(USC/ISI)、麻省理工学院的计算机科



学实验室等联合参与的未来互联网架构研究项目,目的是根据现有的网络实体及未来的网络需求,重新对互联网的体系结构进行思考和探索。

2005年和2006年,美国国家科学基金(NSF)先后启动了关于未来网络的研究计划GENI和FIND。GENI获得了3亿美元的资助,目标是重新设计互联网体系结构,打造一个更适合未来的新一代互联网并为此搭建网络测试环境。FIND的项目资金为2 000万美元,拟从根本上重新设计新一代网络,以解决现有网络在安全性、移动性等方面存在的严重弊端,最终目标是设计一个适合未来15年需求的新一代互联网。

2006年欧盟启动了ANA、BIONETS和Haggle等研究全新网络体系结构的项目。ANA为期4年,参与者为欧洲和北美的大学及研究机构,目标是探索全新的网络架构并设计一种自治的网络。BIONETS同样为期4年,主要参与者包括诺基亚、意大利

电信和瑞士Basel大学等,目标是仿照生物学的思路设计全新网络框架。Haggle的研究周期为2006—2010年,主要参与者包括剑桥大学等。Haggle提出一个新的自治网络架构,支持间歇性连接网络环境,特别是缺乏端到端连接的环境中的自治通信。

在世界各发达国家对未来互联网体系结构和网络技术进行理论探讨的同时,中国的科研工作者也积极开展了这个领域的研究工作。2003年,国家“973”项目开始启动新一代互联网体系结构理论研究的计划。2008,在国家“863”计划项目的资助下中国的研究人员也开始对新型网络架构及协议体系进行了研究和探索,主要目标是在分析现有网络问题的基础上,围绕未来网络通信需求,结合自治计算、自治通信等研究领域的最新技术,研究和提出适应未来网络/业务需求的自治化的新型通信网络体系结构模型。(待续)

收稿日期:2009-05-22

## 作者简介



陆璇,北京邮电大学计算机科学与技术学院在读博士研究生,主要研究方向为互联网体系结构、自治网络。



龚向阳,北京邮电大学网络与交换技术国家重点实验室副教授,主要研究领域为新型互联网体系结构、宽带网络技术与服务质量等。



程时端,北京邮电大学网络与交换技术国家重点实验室教授、博士生导师,主要研究领域为宽带网络、网络性能与服务质量等。

## 中兴通讯发布第一代多业务可重构路由器ZXR10 M6000

【本刊讯】2009年6月16日中兴通讯在新加坡CommunicAsia 2009电信展上发布了第一代多业务可重构路由器ZXR10 M6000。ZXR10 M6000作为电信级多业务路由器,可以部署在大型城域业务边缘,提供丰富的业务接入和强大的业务控制能力,旨在解决运营商全业务运营的关键需求:更高的带宽,更丰富的业务接入,灵活快速的业务部署,更低的总体运营成本(TCO)。

电信业务已经由单一模式逐步向多样性发展,固网运营商和移动运营商也逐步融合业务。业务的融合要求运营商提供统一的承载网络支持各类业务的需求,而支撑统一业务承载网的基础就是设备能力的提升和综合业务承载能力的提供。中兴通讯紧随电信时代的脚步,推出了新一代的电信级融合设备ZXR10 M6000,将BRAS和SR的功能融合,并且可选择配置各种业务模块,统一平台实现多种业务的接入,方便运营商快速开展多种业务。ZXR10 M6000同时可以提供单边缘、双边缘以及宽带接入服务器(BRAS)集中部署等业务汇聚方案,是平滑

演进网络和低TCO网络建设的最佳选择。

中兴通讯承载网产品线副总经理赵强先生介绍:“ZXR10 M6000系列产品是中兴通讯数据产品研发团队秉承10多年来在高端路由器和BRAS的研发经验和运营商的大量的应用案例,研发出全新架构的第一代多业务可重构路由器设备。ZXR10 M6000系列产品可根据在不同建网时期、不同用户规模、不同业务开展情况下的网络重建需要,实现业务可重构、硬件可重构、系统可重构,保持网络的持续、可靠以及业务的平滑升级,同时降低运营商TCO。”

ZXR10 M6000多项突破性的性能指标使得这款新概念路由器得到业界的高度关注。ZXR10 M6000基于高度的模块化和先进的交换结构设计,独创交换网板2+2备份功能,支持业界最大的单向480 Gb/s交换网板,使得整机最大交换容量可达3.84T。ZXR10 M6000采用高性能的网络处理器和专用硬件芯片可实现单板40 Gb/s线速转发,未来可平滑升级至100 Gb/s。ZXR10 M6000采用多种智能节能技术,使得运营商真正实现绿色运维。